

**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ
СПРАВ**

Сумська філія

Кафедра соціально-економічних дисциплін

ТЕКСТ ЛЕКЦІЇ

**з навчальної дисципліни «Інформаційні та комунікаційні технології»
обов'язкових компонент
освітньої програми першого (бакалаврського) рівня вищої освіти**

262 Правоохоронна діяльність (поліцейські)

**за темою – «Інформаційно-аналітичного забезпечення національної
поліції України»**

ЗАТВЕРДЖЕНО

Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 30.08.2023 р № 7

СХВАЛЕНО

Вченою радою Сумської філії
Харківського національного
університету внутрішніх справ
Протокол від 29.08.2023 р № 8

ПОГОДЖЕНО

Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 29.08.2023 р № 7

Розглянуто на засіданні кафедри соціально-економічних дисциплін Протокол від
29.08.2023 р № 2

Розробники:

Доцент кафедри соціально-економічних дисциплін Сумської філії ХНУВС, к.е.н.,
доцент Виганяйло Світлана Миколаївна

Рецензенти:

1. Доцент кафедри протидії кіберзлочинності, факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ, к.п.н., доцент Тетяна
Петрівна Колісник
2. Доцент кафедри кібернетики та інформатики СНАУ, к.е.н., доцент Олександр
Борисович В'юненко

План лекції

1. Вступ. Міжнародно-правові та конституційні засади прав людини в галузі інформації
2. Нормативно-правове регулювання у сфері інформаційних відносин у поліцейській діяльності.
3. Організація інформаційно-аналітичного забезпечення Національної поліції України
4. Система централізованого управління нарядами поліції
5. Висновки

Рекомендована література

Нормативні документи

1. Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII // Відомості Верховної Ради України. – 2015. – № 40-41. – ст. 379 <https://zakon.rada.gov.ua/laws/show/580-19>
2. Закон України “Про захист персональних даних” від 01.06.2010 за 2297-VI. <https://zakon.rada.gov.ua/laws/show/2297-17>
3. Про захист інформації в інформаційно-телекомунікаційних системах. Закон України URL <https://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80>
4. Про затвердження Положення про інформаційно-телекомунікаційну систему “Інформаційний портал Національної поліції України”: Наказ МВС України від 03.08.2017 № 676 URL <https://zakon.rada.gov.ua/laws/show/z1059-17>
5. Про затвердження Положення про єдину інформаційну систему Міністерства внутрішніх справ та переліку її пріоритетних інформаційних ресурсів: Постанова КМУ від 14 листопада 2018 р. № 1024 URL <https://zakon.rada.gov.ua/laws/show/1024-2018-%D0%BF>

Основна

1. Виганяйло С. М. Інформаційне забезпечення професійної діяльності: навч. посіб. Харків: ХНУВС, 2021. 110 с.
2. Клімушин П. С. Інформаційні системи та технології в економіці : навчальний посібник / П. С. Клімушин, О. В. Орлов, А. О. Серенок; Нац. акад. держ. управління при Президентові України, Харк. регіон. ін-т держ. управління. - Харків : Вид-во ХарПІ НАДУ "Магістр", 2011. - 448 с <http://dspace.univd.edu.ua/xmlui/handle/123456789/4730>
3. Сезонова І. К. Інформатика для правоохоронців: навч. посіб. / І. К. Сезонова; МВС України, Харк. нац. ун-т внутр. справ. - Харків, 2015. – 182 с. <http://dspace.univd.edu.ua/xmlui/handle/123456789/1311>

Допоміжна

1. Вишня В. Б. Основи інформаційної безпеки: навч. посіб. / В.Б. Вишня, О.С. Гавриш, Е.В. Рижков. Дніпро: ДДУВС, 2020. 128 с. <http://er.dduvs.in.ua/handle/123456789/4206>
2. Заплотинський Б.А. Інформаційні технології в юридичній діяльності.

- Посібник. Київський інститут інтелектуальної власності та права НУ “Одеська юридична академія”, кафедра інформаційно-аналітичної та інноваційної діяльності, 2018.–108с.
3. Застосування інформаційних технологій у діяльності правоохоронних органів : зб. матеріалів кругл. столу (м. Харків, 9 груд. 2020 р.) / МВС України, Харків. нац. ун-т внутр. справ. – Харків : ХНУВС, 2020. – 132 с. <http://dspace.univd.edu.ua/xmlui/handle/123456789/9984>
<http://dspace.onua.edu.ua/bitstream/handle/11300/11095/%D0%86%D0%A2%20%D0%B2%20%D0%AE%D0%94%20%D0%BF%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA.pdf?sequence=1&isAllowed=y>
 4. Інформаційне забезпечення юридичної діяльності : підручник / В.Б. Вишня, Л.В. Рибальченко, О.О. Косиченко та ін.; за заг. ред. В.Б. Вишні; МВС України, Дніпропетр. держ. ун-т внутр. справ.- Дніпро : ДДУВС, 2019.- 227 с. <http://er.dduvs.in.ua/handle/123456789/3718>
 5. Інформаційне забезпечення діяльності Національної поліції України: зб. законодавчих та нормативних документів / уклад.:В.Б. Вишня та ін. Дніпро: ДДУВС, 2016. 476 с. <http://er.dduvs.in.ua/handle/123456789/2043>
 6. Кормич Б.А., Федотов О.П., Аверочкина Т.В. Правове регулювання інформаційної діяльності: навчально-методичний. Одеська юридична академія. 2018. 150 с.
https://pidruchniki.com/15931106/politologiya/pravove_regulyuvannya_informatsiynoyi_sferi_ukrayini
 7. Краснобрижий І.В. Інформаційне забезпечення професійної діяльності : навч. посіб. Уклад: І.В. Краснобрижий, С.О. Прокопов, Е.В. Рижков. Дніпро : ДДУВС, 2018. 220 с. <http://er.dduvs.in.ua/handle/123456789/2046>
 8. Методичні рекомендації щодо використання комп'ютерної програми «Навчальний ЄРДР» (для ролі «курсант») / [Розроб. Коршенко В. А., Демидов З. Г., Колмик О. О., Абламський С. Є.]; МВС України, Харків. нац. ун-т внутр. справ, Наук.-досл. лаб. з проблем розвитку інформац. технологій, Каф. крим. процесу та організації досуд. слідства ф-ту № 1. - Харків: ХНУВС, 2019. - 30 с.
<http://dspace.univd.edu.ua/xmlui/handle/123456789/6675>
 9. Мордвинцев М. В. Використання автоматизованих систем відеодокументування переміщень об'єкта для протидії торгівлі людьми / М. В. Мордвинцев, О. В. Хлестков, С. П. Ницюк // Використання сучасних інформаційних технологій в діяльності Національної поліції України: матеріали Всеукр. наук.-практ. семінару (м. Дніпро, 23 листоп. 2018 р.). – Дніпро: Дніпропетр. держ. ун-т внутріш. справ, 2018. – С. 52-54. <http://dspace.univd.edu.ua/xmlui/handle/123456789/3953>
 10. Наказ МВС “Про затвердження Положення про Інтегровану інформаційно-пошукову систему ОВС України” від 12.10.2009 за № 436. <http://tranzit.ltd.ua/nakaz/>
 11. Наказ МВС “Про затвердження Положення про систему Інтернет у телекомунікаційній мережі Національної поліції України” від 22.02.2017 № 141. <http://tranzit.ltd.ua/nakaz/>

12. Нелюбов В.О., Куруца О.С. Основи інформатики. Microsoft Word 2016: електронний навчальний посібник. Ужгород: ДВНЗ УжНУ, 2018. 96 с. <https://dspace.uzhnu.edu.ua/jspui/handle/lib/18659>
13. Про електронні довірчі послуги: Закон України від 5 жовтня 2017 р. № 2155-VIII. URL: <http://zakon2.rada.gov.ua/laws/show/2155-19/page>
14. Проведення оперативно-тактичних навчань на основі інформаційного моделювання дій нарядів та інших підрозділів Національної поліції : методичні рекомендації / О.О. Акімова, О.С. Гавриш, О.В. Махницький, С.О. Прокопов, Е.В. Рижков, Ю.І. Тюрня. Дніпро: Дніпроп. держ. ун-т. внутр. справ, 2017. 37 с. <https://dduvs.in.ua/wp-content/uploads/files/Structure/library/student/eib2.pdf>

Інформаційні ресурси в Інтернеті

1. <http://www.nau.kiev.ua>
2. <http://www.liga.kiev.ua>
3. <http://www.informjust.kiev.ua>
4. <http://www.rada.gov.ua>
5. <https://zakon.rada.gov.ua>
6. <http://www.president.gov.ua>

Текст лекції

1. Вступ. Міжнародно-правові та конституційні засади прав людини в галузі інформації

У другій половині ХХ ст. утвердилися наднаціональні, міжнародні засоби захисту прав людини, які спиралися на розуміння того, що додержання прав людини не може вважатися внутрішньою справою держави. Конституційними засадами прав людини в сфері інформації є статті 3, 32, 34, 40. Вони підкріплюються нормами статей 15, 21, 28, 41 та ін. Згідно з нормами ч. 3 ст. 55 Конституції України створено реальні правові передумови для більш ефективного захисту громадянами своїх прав. Головним міжнародно-правовим стандартом у галузі прав людини є Хартія про права людини, що складається із Загальної декларації прав людини, Міжнародного пакту про економічні, соціальні і культурні права та Міжнародного пакту про громадянські та політичні права. Ці акти є головним стандартом, на основі якого було розроблено низку інших міжнародних та національних правових актів в галузі прав людини. Правовий статус людини як суб'єкта інформаційних відносин ґрунтується на двох основних правах: 1) право вільно, безперешкодно, на власний розсуд бути суб'єктом інформаційних процесів, шукати, одержувати і поширювати інформацію, яке не пов'язане з територіальною юрисдикцією держави і не обмежується територіально державними кордонами; 2) це право на захист від неправомірного інформаційного втручання (privacy), тобто право на конфіденційність інформації про особисте життя та на захист від розповсюдження вигаданої й перекрученої інформації, що завдає шкоди честі й репутації особи.

Підстави та випадки обмеження прав людини в галузі інформації. Характеристика правового засад (міжнародних і національних) та головних умов обмеження прав людини у сфері інформації. Групи випадків та причин

обмеження реалізації інформаційних прав людини: 1) необхідні для захисту безпеки держави: охорона, захист громадського порядку, громадської безпеки, національної безпеки, територіальної цілісності; 2) необхідні для захисту здоров'я населення та моральних засад; 3) необхідні для забезпечення та захисту: прав і свобод людини, конфіденційності особистого життя, репутації людини, інтересів малолітніх; 4) для запобігання заворушенням або злочинам, забезпечення інтересів правосуддя, підтримання авторитету і неупередженості правосуддя, запобігання розголошенню інформації, одержаної конфіденційно; 5) права держави та її компетентних органів вводити певні процедури щодо ліцензування мас-медіа.

Захист від негативного інформаційного впливу. Засоби інформаційно-психологічного захисту людини включають наступні рівні: 1) суспільний рівень, коли захист реалізується шляхом регулювання інформаційних потоків у системі розповсюдження масової інформації, а також застосуванням відповідних способів, методів і засобів обробки та оцінки інформації в процесі соціальної взаємодії. Суб'єктами захисту на цьому рівні є держава і суспільство через діяльність певних соціальних інститутів (системи освіти, системи поширення духовних і культурних цінностей, традицій, соціальних норм тощо). 2) Груповий рівень, коли захист реалізується за допомогою поширення й використання внутрішньо-групових інформаційних джерел і потоків, а також специфічних для конкретних соціальних груп та організацій способів взаємодії, переробки та оцінки інформації. На цьому рівні суб'єктами психологічного захисту є соціальні групи та організації (сім'я, суспільні, політичні, релігійні та інші об'єднання). 3) На особистому рівні захист реалізується на основі специфічних механізмів вольової поведінки, які утворюють систему індивідуального інформаційно-психологічного захисту. На цьому рівні розрізняються механізми особистого захисту від внутрішніх і зовнішніх негативних інформаційних впливів.

Доступ до публічної інформації. Публічна інформація може відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених Законом «Про доступ до публічної інформації».

Публічна інформація з обмеженим доступом класифікується на конфіденційну, таємну, службову інформацію. Вимоги до обмеження доступу до інформації: 1) виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку; 2) розголошення інформації може завдати істотної шкоди цим інтересам; 3) шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

Розпорядники публічної інформації відповідно до Закону України від 13.01.2011 р. «Про доступ до публічної інформації» зобов'язані: 1) оприлюднювати інформацію про свою діяльність та прийняті рішення; 2) систематично вести облік документів, що знаходяться в їхньому володінні; 3)

вести облік запитів на інформацію; 4) визначати спеціальні місця для роботи запитувачів з документами чи їх копіями, а також надавати право запитувачам робити виписки з них, фотографувати, копіювати, сканувати їх, записувати на будь-які носії інформації тощо; 5) мати спеціальні структурні підрозділи або призначати відповідальних осіб для забезпечення доступу запитувачів до інформації; 6) надавати достовірну, точну та повну інформацію, а також у разі потреби перевіряти правильність та об'єктивність наданої інформації. Розпорядник також повинен: своїм рішенням визначити особу (осіб), відповідальну за здійснення контролю за обліком документів у розпорядника, при цьому бажано, щоб це не були особи, відповідальні за оброблення інформаційних запитів, оскільки ці дві функції є відмінними і вимагають значних витрат часу і спеціалізації; розробити і затвердити внутрішнє положення про облік документів, що знаходяться у володінні розпорядника.

Гарантії доступу до публічної інформації. Право на доступ до публічної інформації гарантується: 1) обов'язком розпорядників інформації надавати та оприлюднювати інформацію, крім випадків, передбачених законом; 2) визначенням розпорядником інформації спеціальних структурних підрозділів або посадових осіб, які організовують у встановленому порядку доступ до публічної інформації, якою він володіє; 3) максимальним спрощенням процедури подання запиту та отримання інформації; 4) доступом до засідань колегіальних суб'єктів владних повноважень, крім випадків, передбачених законодавством; 5) здійсненням парламентського, громадського та державного контролю за дотриманням прав на доступ до публічної інформації; 6) юридичною відповідальністю за порушення законодавства про доступ до публічної інформації.

Оприлюднення публічної інформації. Доступ до інформації забезпечується шляхом систематичного та оперативного оприлюднення інформації: в офіційних друкованих виданнях; на офіційних веб-сайтах в мережі Інтернет; на інформаційних стендах; будь-яким іншим способом.

Інформаційна безпека та інформаційна політика держави. В інформаційній безпеці виділяються три комплекси питань, які диференціюються відповідно до природи правових норм, що становлять їх нормативно-правову базу: 1) інформаційна безпека людини і суспільства, яка ґрунтується, передусім на нормах природного права і вимірюється ступенем свободи від втручання держави та інших осіб, можливостями самореалізації та самовизначення; 2) інформаційна безпека держави, що ґрунтується на позитивному праві і пов'язана із застосуванням обмежень, заборон, жорсткою регламентацією. Невід'ємним її елементом є сила державного примусу; 3) інформаційна безпека суб'єктів підприємницької діяльності, яка насамперед має бути визначена законодавством з питань захисту конкуренції, регулювання економіки тощо. *Основні способи реалізації державної політики у сфері інформаційної безпеки:* розроблення нормативно-правових актів, створення нових державних інституцій та розширення компетенції існуючих у сфері інформаційної безпеки; застосування конкретних, установлених правовими нормами засобів і напрямів державного впливу на інформаційну сферу.

Захист персональних даних. Особливості правового режиму інформаційних систем з обробки персональних даних.

Конституція України визначає доступ до персональних даних як обов'язкову умову згоди особи на збирання, зберігання, використання та розповсюдження інформації про приватне життя особи. Під інформаційними системами персональних даних розуміється сукупність персональних даних, які містяться в базах даних і інформаційних технологіях та технічних засобах, що забезпечують їх оброблення.

Використовуючи інформаційні технології та маючи певний набір персональних даних, що використовується приватними особами для управління своїми матеріальними та фінансовими ресурсами, можна отримати неправомірний доступ та права на володіння цим ресурсом. Розвиток різних інформаційних систем, зокрема і відкритих, має одну із своїх цілей захисту від витоків даних і запобігання несанкціонованому доступу до інформації персонального характеру. Це актуалізує та збільшує значущість різноманітних засобів захисту інформації технічними та законодавчими засобами.

Законодавством України не встановлено і не може бути встановлено чіткого переліку відомостей про фізичну особу, які є персональними даними, в тому числі при обробці персональних даних в інформаційних (автоматизованих) базах та картотеках персональних даних, що можуть виникнути у майбутньому, у зв'язку зі зміною в технологічній, соціальній, економічній та інших сферах суспільного життя.

Правове регулювання інформаційних баз даних, що містять персональні дані, база даних за своєю правовою природою є ширшим поняттям, ніж база персональних даних, включає сукупність взаємопов'язаних і систематизованих загальних елементів, що в сукупності утворюють базу даних. Своєю чергою, база персональних даних включає тільки окремий вузлий напрям – персональні дані. За таких обставин база даних як ширше поняття може включати персональні дані в сукупності з іншими елементами, а база персональних даних – лише сукупність даних у сфері оброблення даних фізичних осіб. У контексті формування інформаційних баз даних доцільно розділити персональні дані ідентифікації та персональні дані, які характеризують особу.

Суб'єктів правовідносин у сфері персональних даних можна розділити на категорії: суб'єкти, що надають персональні дані – фізичні особи; суб'єкти, які проводять обробку персональних даних (оператори); суб'єкти, що передають персональні дані; суб'єкти, що використовують оброблені персональні дані.

Оператори, незалежно від їх відомчої приналежності, повинні залучати до обслуговування інформаційних систем (зберігання, обробки та видачі персональних даних) спеціально навчених осіб і мати дозволи (ліцензії) на роботу з таким типом систем. Законодавчо встановлені заходи відповідальності за неправомірні дії з персональними даними, але немає диференціації залежно від того, які дані піддавали неправомірній обробці, розголошенню тощо. Необхідність зберігання та обробки персональних даних з урахуванням їх згаданої категоризації в автоматизованих інформаційних системах зумовлюють

необхідність застосування спеціальних правових режимів у відношенні інформаційних систем, що забезпечують зберігання та обробку.

Інформаційна система для обробки персональних даних – це сукупність персональних даних, що містяться в базі даних, інформаційних технологій і технічних засобів, що дають змогу здійснювати обробку персональних даних з використанням засобів автоматизації. Обробка персональних даних в інформаційних системах представляє дію або сукупність дій, що здійснюються з використанням засобів автоматизації із персональними даними, включаючи збирання, записування, систематизацію, накопичення, зберігання, уточнення (оновлення, зміна), вилучення, використання, передачу (розповсюдження, надання, доступ), знеособлення, видалення, знищення персональних даних.

Обробка персональних даних в інформаційних системах повинна відповідати таким принципам обробки: законна та справедлива основа; обробка повинна обмежуватися досягненням конкретних, певних і законних цілей. Загальним правилом обробки персональних даних в Європейському Союзі є наявність угод суб'єкта даних на їх обробку. Будь-який виняток має бути передбачено законами. Наприклад, відповідно до законодавства обробка персональних даних може продовжуватися після відкликання згоди суб'єктом, навіть якщо йдеться про спеціальні категорії персональних даних, що стосуються расової, національної приналежності, політичних поглядів, релігійних чи філософських переконань, стану здоров'я, інтимного життя у випадках, передбачених у п. 7 ч. 2 ст. 7 «Особливі вимоги до обробки персональних даних» Закону України «Про захист персональних даних».

Однією з основних причин актуальності внутрішніх загроз інформаційній безпеці є несанкціонований витік інформації за межі захищених інформаційних систем, обсяг якої має сталу тенденцію до зростання. Опинившись за межами захищеної інформаційної системи, персональні дані стають доступними практично необмеженому колу користувачів і можуть бути знищені чи спотворені, а також можуть бути використані з метою завдання шкоди особі, якої стосуються і моральної і матеріальної. Практично всі органи державної влади створюють і працюють з інформаційними системами персональних даних і зобов'язані забезпечити їх конфіденційність. У більшості цих органів діють внутрішні акти, що регулюють правила обробки персональних даних і встановлюють коло осіб, допущених до такої обробки, та відповідальність за порушення режиму захисту.

Відповідно до Типового порядку обробки персональних даних головними критеріями у забезпеченні захисту є вміст і обсяг персональних даних; актуальність загрози; ознака того, чи є співробітник оператором чи ні. Шкода суб'єкта та види діяльності оператора і не розглядаються. Актуальним, але не зрозумілим з боку безпосереднього застосування, є введення низки дефініцій, зокрема автоматизованої системи.

Сьогодні можна виділити низку організаційно-технічних проблем, спрямованих на забезпечення безпеки персональних даних в інформаційних системах.

По-перше, оскільки не є загальнодоступними персональні дані, які належать до категорії конфіденційної інформації, для здійснення заходів захисту необхідно отримати ліцензію Державної служби спеціального зв'язку та захисту інформації України на діяльність у галузі технічного захисту конфіденційної інформації. Під час використання засобів криптографічного захисту інформації також необхідна наявність ліцензій. Водночас отримання зазначених ліцензій вимагає від організації наявності висококваліфікованого персоналу, спеціального обладнання та приміщень, що часто є нелегким завданням для працівників багатьох організацій.

Іншою проблемою є безпрецедентно високі вимоги, що висуваються до системи захисту. Наприклад, рівень захисту для деяких інформаційних систем персональних даних відповідає рівню захисту державної таємниці. Зокрема обов'язковим є забезпечення захисту інформації від витоків за рахунок електромагнітних випромінювань і наведень від засобів обчислювальної техніки та ліній зв'язку. Також слід враховувати, що до такого класу належать системи, в яких обробляється велика кількість інформації та системи, в яких обробляються спеціальні категорії персональних даних.

Існує низка підходів, що дають змогу забезпечити захист персональних даних відповідно до вимог ціною розумних витрат. Насамперед знизити витрати на побудову системи захисту можна шляхом вибору архітектури самої інформаційної системи на етапі її проектування. Наприклад, поділ великої інформаційної системи персональних даних на кілька територіальних дозволяє скоротити кількість персональних даних, оброблюваних у кожній системі, а використання умовних ідентифікаторів дає можливість обмежити доступ до даних.

Особливу зацікавленість з погляду «архітектури» побудови систем набуває технологія термінального доступу, при якій вся обробка даних здійснюється на сервері, а робочі станції використовуються тільки для відображення інформації і отримання даних від користувача. За правильного використання подібний підхід дозволяє заощадити на засобах захисту і атестації за вимогами безпеки. Водночас зменшуються витрати на управління інформаційною інфраструктурою та закупівлю засобів обчислювальної техніки за рахунок централізації системи і зниження вимог до апаратних характеристик комп'ютерів користувачів.

Основною причиною правопорушень у цій сфері є неправомірне поширення персональних даних. У більшості випадків порушником є оператор персональних даних – державний орган, орган місцевого самоврядування, юридична або фізична особа, що організують і здійснюють обробку персональних даних, визначають цілі та зміст обробки персональних даних.

2. Нормативно-правове регулювання у сфері інформаційних відносин у поліцейській діяльності.

Стаття 25. Повноваження поліції у сфері інформаційно-аналітичного забезпечення

Поліція здійснює інформаційно-аналітичну діяльність виключно для реалізації своїх повноважень, визначених цим Законом «Про Національну поліцію».

Поліція в рамках інформаційно-аналітичної діяльності:

- формує бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України;
- користується базами (банкami) даних Міністерства внутрішніх справ України та інших органів державної влади;
- здійснює інформаційно-пошукову та інформаційно-аналітичну роботу;
- здійснює інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями.

Поліція може створювати власні бази даних, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу, а також міжвідомчі інформаційно-аналітичні системи, необхідні для виконання покладених на неї повноважень.

Діяльність поліції, пов'язана із захистом і обробкою персональних даних, здійснюється на підставах, визначених Конституцією України, Законом України «Про захист персональних даних», іншими законами України.

Стаття 26. Формування інформаційних ресурсів поліцією

Поліція наповнює та підтримує в актуальному стані бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України, стосовно:

- осіб, щодо яких поліцейські здійснюють профілактичну роботу;
- виявлених кримінальних та адміністративних правопорушень, осіб, які їх учинили, руху кримінальних проваджень; обвинувачених, обвинувальний акт щодо яких направлено до суду;
- розшуку підозрюваних, обвинувачених (підсудних) осіб, які ухиляються від відбування покарання або вироку суду;
- розшуку безвісно зниклих;
- установлення особи невпізнаних трупів та людей, які не можуть надати про себе будь-яку інформацію у зв'язку з хворобою або неповнолітнім віком;
- зареєстрованих в органах внутрішніх справ кримінальних або адміністративних правопорушень, подій, які загрожують особистій чи публічній безпеці, надзвичайних ситуацій;
- осіб, затриманих за підозрою у вчиненні правопорушень (адміністративне затримання, затримання згідно з дорученнями органів правопорядку, затримання осіб органами досудового розслідування, адміністративний арешт, домашній арешт);
- осіб, які скоїли адміністративні правопорушення, провадження у справах за якими здійснюється поліцією;

- зареєстрованих кримінальних та адміністративних корупційних правопорушень, осіб, які їх учинили, та результатів розгляду цих правопорушень у судах;
- іноземців та осіб без громадянства, затриманих поліцією за порушення визначених правил перебування в Україні;
- викрадених номерних речей, цінностей та іншого майна, які мають характерні ознаки для ідентифікації, або речей, пов'язаних із учиненням правопорушень, відповідно до заяв громадян;
- викрадених (втрачених) документів за зверненням громадян;
- знайдених, вилучених предметів і речей, у тому числі заборонених або обмежених в обігу, а також документів з ознаками підробки, які мають індивідуальні (заводські) номери;
- викрадених транспортних засобів, які розшукуються у зв'язку з безвісним зникненням особи, виявлених безгосподарних транспортних засобів, а також викрадених, втрачених номерних знаків;
- виданих дозвільних документів у сфері безпеки дорожнього руху та дозволів на рух окремих категорій транспортних засобів;
- зброї, що перебуває у володінні та користуванні фізичних і юридичних осіб, яким надано дозвіл на придбання, зберігання, носіння, перевезення зброї;
- викраденої, втраченої, вилученої, знайденої зброї, а також добровільно зданої зброї із числа тієї, що незаконно зберігалася;
- бази даних, що формуються в процесі здійснення оперативно-розшукової діяльності відповідно до закону.

Під час наповнення баз (банків) даних, визначених у пункті 7 частини першої цієї статті, поліція забезпечує збирання, накопичення мультимедійної інформації (фото, відео-, звукозапис) та біометричних даних (дактилокартки, зразки ДНК).

Стаття 27. Використання поліцією інформаційних ресурсів

Поліція має безпосередній оперативний доступ до інформації та інформаційних ресурсів інших органів державної влади за обов'язковим дотриманням Закону України «Про захист персональних даних».

Інформація про доступ до бази (банку) даних повинна фіксуватися та зберігатися в автоматизованій системі обробки даних, включно з інформацією про поліцейського, який отримав доступ, та про обсяг даних, доступ до яких було отримано.

Кожна дія поліцейського щодо отримання інформації з інформаційних ресурсів, передбачених статтями 26, 27 цього Закону, фіксується у спеціальному електронному архіві, ведення якого покладається на службу інформаційних технологій Міністерства внутрішніх справ України.

В електронному архіві фіксуються прізвище, ім'я, по батькові та номер спеціального жетона поліцейського, вид отриманої інформації, реєстр, з якого отримувалася інформація, час отримання інформації та інші дані, необхідні для ідентифікації поліцейського, який отримував інформацію з реєстрів.

Стаття 28. Відповідальність за протиправне використання інформаційних ресурсів

Поліція вживає всіх заходів для недопущення будь-яких порушень прав і свобод людини, пов'язаних з обробкою інформації.

Поліцейські несуть персональну дисциплінарну, адміністративну та кримінальну відповідальність за вчинені ними діяння, що призвели до порушень прав і свобод людини, пов'язаних з обробкою інформації.

Міністерство внутрішніх справ України у межах компетенції здійснює контроль за дотриманням вимог законів та інших нормативно-правових актів під час формування та користування поліцейськими інформаційними базами (банками) даних у порядку, визначеному у статтях 26, 27 цього Закону.

Стаття 40. Застосування технічних приладів та технічних засобів, що мають функції фото- і кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису

Поліція для забезпечення публічної безпеки і порядку може закріплювати на форменому одязі, службових транспортних засобах, монтувати/розміщувати по зовнішньому периметру доріг і будівель автоматичну фото- і відеотехніку, а також використовувати інформацію, отриману із автоматичної фото- і відеотехніки, що знаходиться в чужому володінні, з метою:

- попередження, виявлення або фіксування правопорушення, охорони громадської безпеки та власності, забезпечення безпеки осіб;
- забезпечення дотримання правил дорожнього руху.

Інформація про змонтовану/розміщену автоматичну фототехніку і відеотехніку повинна бути розміщена на видному місці.

3. Організація інформаційно-аналітичного забезпечення Національної поліції України

З метою організації інформаційно-аналітичного забезпечення поліції було розроблено Положення про інформаційно-телекомунікаційна систему «Інформаційний портал Національної поліції України». Інформаційно-телекомунікаційна система «Інформаційний портал Національної поліції України» (далі - система ІПНП) - сукупність технічних і програмних засобів, призначених для обробки відомостей, що утворюються у процесі діяльності Національної поліції України та її інформаційно-аналітичного забезпечення.

Розглянемо основні завдання системи «Інформаційний портал Національної поліції України», до них належать:

- інформаційно-аналітичне забезпечення діяльності Національної поліції України;
- забезпечення наповнення та підтримки в актуальному стані інформаційних ресурсів баз (банків) даних, що входять до ЄІС МВС;
- забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу;
- забезпечення електронної взаємодії з МВС та іншими органами державної влади.

Система «Інформаційний портал Національної поліції України» призначена для:

- формування інформаційних ресурсів ЄІС МВС;
- обробки інформації, яка утворена в процесі діяльності поліції; □ надання безпосереднього оперативного доступу до інформаційних ресурсів ЄІС МВС;
- генерації інтерфейсів та оброблення тимчасових наборів даних для здійснення інформаційної взаємодії органів (підрозділів) поліції з іншими органами державної влади, органами правопорядку іноземних держав, міжнародними організаціями;
- здійснення пошукових та аналітичних функцій для використання інформації з інформаційних ресурсів (баз даних) поліції, МВС та інших органів державної влади в межах службової діяльності відповідно до рівня доступу і повноважень за запитом або регламентом;
- використання програмних компонентів геоінформаційних підсистем для візуалізації інформації у вигляді електронних карт, автоматичної зміни зображеного образу об'єкта в залежності від зміни його характеристик, зміни масштабу та деталізації картографічної інформації в інформаційних ресурсах;
- забезпечення автоматизації процесів управління силами та засобами поліції;
- забезпечення електронного документообігу в органах (підрозділах) поліції, обміну електронними документами з МВС;
- комплексного захисту інформації та розмежування доступу до інформації, що зберігається в базах даних системи «Інформаційний портал Національної поліції України».

В інформаційних ресурсах системи «Інформаційний портал Національної поліції України» обробляється інформація, яка належить до державних інформаційних ресурсів. Така інформація не підлягає поширенню та передачі іншим особам, крім випадків, передбачених законодавством. Інформаційними ресурсами системи ІПП є інформація, що утворена в процесі діяльності поліції та використовується для формування:

- тимчасових наборів даних, що створюються в процесі діяльності поліції та використовуються для наповнення та підтримки в актуальному стані баз (банків) даних, які входять до ЄІС МВС та визначені статтею 26 Закону України «Про Національну поліцію»;
- баз даних у сфері управлінських відносин, необхідних для виконання покладених на поліцію повноважень;
- баз даних, необхідних для забезпечення щоденної діяльності поліції, у сфері трудових відносин, фінансового забезпечення, документообігу.

Бази даних поліції, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції, містять відомості, зокрема, стосовно:

- повідомлень про кримінальні та адміністративні правопорушення, надзвичайні ситуації та інші події, що надійшли технічними каналами зв'язку;
- щодобових переліків та складу нарядів поліції та слідчо-оперативних груп, що заступають на чергування; □ завдань та орієнтувань, що доводились

до нарядів поліції для реагування на повідомлення про кримінальні та адміністративні правопорушення, надзвичайні ситуації та інші події;

- звітування нарядів поліції за результатами реагування на повідомлення про кримінальні та адміністративні правопорушення, надзвичайні ситуації та інші події, виявлення додаткових обставин на місці пригоди;

- пересувань нарядів поліції, які отримані із планшетних комп'ютерів (мобільних терміналів) та засобами GPS. Поліція може створювати інші бази даних, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції, відповідно до статті 25 Закону України «Про Національну поліцію».

Розпорядником системи «Інформаційний портал Національної поліції України» є Національна поліція України, який вживає заходів із організації матеріально-технічного та кадрового забезпечення, що необхідні для ефективного функціонування системи. Адміністратором системи ІПП є уповноважений структурний підрозділ апарату центрального органу управління Національної поліції України, який забезпечує:

- вирішення організаційних питань щодо забезпечення функціонування системи;

- ведення обліку користувачів та надання їм доступу до інформації, що в ній обробляється;

- захист інформації від несанкціонованого доступу, знищення, модифікації та блокування доступу до неї шляхом здійснення організаційних і технічних заходів, впровадження засобів та методів технічного захисту інформації;

- вжиття заходів стосовно розвитку і вдосконалення системи;

- координацію функціонування складових системи.

Користувачами системи «Інформаційний портал Національної поліції України» є посадові особи органів (підрозділів) поліції, яким в установленому порядку надано право доступу до інформації в цій системі. Ідентифікація користувача та підтвердження цілісності даних, що обробляються в системі ІПП, забезпечуються застосуванням електронного цифрового підпису або інших програмно-технічних засобів авторизації користувачів та забезпечення цілісності даних. Кожна дія користувача щодо отримання інформації з інформаційних ресурсів системи «Інформаційний портал Національної поліції України» фіксується у спеціальному електронному архіві. Користувачі системи ІПП зобов'язані не розголошувати у будь-який спосіб інформацію, яка їм стала відома у зв'язку з виконанням посадових обов'язків, крім випадків, передбачених законом, відповідають за достовірність інформації, що вводиться ними до відповідних інформаційних ресурсів системи «Інформаційний портал Національної поліції України», та зобов'язані дотримуватися законодавства у сфері захисту інформації.

Складові системи «Інформаційний портал Національної поліції».

Складовими системи «Інформаційний портал Національної поліції України» є:

- центральний програмно-технічний комплекс;
- автоматизовані робочі місця користувачів;
- телекомунікаційна мережа доступу;
- комплексна система захисту інформації.

Центральний програмно-технічний комплекс системи «Інформаційний портал Національної поліції України» - це сукупність технічних і програмних засобів, призначених для обробки інформації, які забезпечують:

- введення, записування, зберігання, видалення, знищення, приймання та передавання інформації та формування баз даних у системі «Інформаційний портал Національної поліції України»;
- формування тимчасових наборів даних для наповнення та підтримки в актуальному стані інформаційних ресурсів баз (банків) даних ЄІС МВС;
- моніторинг стану інформаційного обміну між складовими системи ПНП, а також системних журналів аудиту роботи користувачів, технічних і програмних засобів;
- захист інформації під час її обробки.

До складу центрального програмно-технічного комплексу системи «Інформаційний портал Національної поліції України» входять:

- центральне сховище даних - програмно-технічний комплекс, який складається із серверів, систем керування базами даних та іншого програмного забезпечення, призначених для безперервного виконання операцій, записування, зберігання, знищення, приймання та передавання інформації, зберігання системних журналів аудиту роботи користувачів та системних журналів реєстрації роботи програмних засобів;
- сервери додатків - програмно-технічний комплекс, який складається із серверів та програмного забезпечення, призначених для безперервного виконання операцій з інформаційного обміну між складовими системи ПНП, функціонування програмних засобів генерації інтерфейсів користувачів для оброблення інформації, записування та зберігання системних журналів аудиту приймання та передавання інформації, реєстрації роботи програмних засобів;
- шлюзові сервери - програмно-технічний комплекс, який складається із серверів, призначених для забезпечення захисту інформації під час здійснення обміну інформацією між підсистемами, взаємодії з інформаційними системами МВС та інших центральних органів виконавчої влади;
- автоматизоване робоче місце адміністратора безпеки - складова комплексної системи захисту інформації в системі ПНП, обладнана технічними засобами та програмним забезпеченням, призначеними для моніторингу системних журналів реєстрації роботи програмних та технічних засобів, аналізу порушень в роботі системи ПНП, налагодження параметрів, необхідних для забезпечення стабільної роботи програмних та технічних засобів, визначення повноважень користувачів системи ПНП.

Центральний програмно-технічний комплекс системи «Інформаційний портал Національної поліції України» розміщується в спеціалізованих службових приміщеннях Національної поліції України.

Розглянемо автоматизовані робочі місця користувачів - це робочі місця поліцейських та інших працівників поліції, обладнані комп'ютерною технікою, у тому числі планшетними комп'ютерами, що підключені до телекомунікаційної мережі доступу системи «Інформаційний портал Національної поліції України» і призначені для автоматизації службової діяльності, реалізації повноважень обробляти інформацію відповідно до наданого рівня доступу в системі ПІНП.

Телекомунікаційна мережа доступу системи «Інформаційний портал Національної поліції України» - сукупність технічних і програмних засобів, призначених для обміну інформацією між складовими системи. Для захисту інформації, що обробляється органами (підрозділами) поліції в системі ПІНП, використовуються канали Єдиної цифрової відомчої телекомунікаційної мережі Міністерства внутрішніх справ України, а при використанні відкритих каналів - засоби захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації.

Комплексна система захисту інформації з підтвердженою відповідністю - взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації. Завданням комплексної системи захисту інформації є забезпечення конфіденційності (у разі обробки інформації з обмеженим доступом), цілісності, доступності інформації в системі «Інформаційний портал Національної поліції України» шляхом здійснення заходів, спрямованих на захист інформації від несанкціонованих дій (у тому числі з використанням комп'ютерних вірусів), які можуть призвести до її випадкової або умисної модифікації чи знищення.

До складу Єдиної інформаційної системи Міністерства внутрішніх справ входять:

Інтегрована інформаційно-пошукова система Національної поліції.

Система централізованого управління нарядами патрульної поліції «ЦУНАМІ»

ДБД Арсенал – відомості щодо зброї, яка перебуває на озброєнні МВС, МО, МНС, АДПС, СБУ, ДПА, ДМС, ДДПВП, УДО.

ІС Оріон – єдині оперативні обліки, які передбачені Законом України „Про оперативно-розшукову діяльність”.

ОДК – оперативно-довідкова картотека, в якій розміщено відомості щодо притягнення осіб до кримінальної відповідальності та судимості осіб.

АДІС "ДАКТО"- автоматична дактилоскопічна інформаційна система.

Складові центрального ПТК ПІНП повинні забезпечити генерацію інтерфейсів, оброблення тимчасових наборів та формування інформаційних ресурсів ЄІС МВС для наступних підсистем:

1) ПІ «Єдиний облік» – автоматизований облік заяв і повідомлень про вчинені кримінальні правопорушення та інші події, зареєстрованих органами Національної поліції України, у тому числі їх структурними (відокремленими) підрозділами (управліннями, відділами, відділеннями), а також організація

контролю за дотриманням порядку веденням цього обліку відповідно до Інструкції (п.1.4.3.2);

2) ІІ «Кримінальна статистика» – автоматизований облік відомостей про кримінальні правопорушення, осіб, які їх учинили або підозрюються в їх учиненні, досудове розслідування за якими здійснюється слідчими органів поліції. Ведення обліку регламентовано Положенням (п. 1.4.3.3);

3) ІІ «Адміністративна практика» – автоматизований облік відомостей щодо зареєстрованих в органах поліції адміністративних правопорушень, осіб, які їх учинили, результатів розгляду цих правопорушень та виконання накладених стягнень у вигляді штрафів та обмін даними про виписки з рахунків надходжень державного бюджету щодо адміністративних штрафів між інформаційною підсистемою «бюджетна установа МВС» та системою ІПНП. Ведення обліку регламентовано інструкціями (п.п. 1.4.3.14, 1.4.3.15, 1.4.3.16);

4) ІІ «Корупція» – автоматизований облік даних стосовно всіх зареєстрованих кримінальних та адміністративних корупційних правопорушень, осіб, які їх учинили, та результатів розгляду цих правопорушень у судах. Ведення обліку регламентовано Інструкцією (п.1.4.3.4);

5) ІІ «Особа» («Правопорушник» та «Підсудний») – автоматизований облік інформації про осіб, щодо яких поліцейські здійснюють профілактичну роботу, а також про обвинувачених осіб, обвинувальний акт щодо яких направлено до суду;

6) ІІ «Розшук» – автоматизований облік відомостей щодо розшуку підозрюваних, обвинувачених (підсудних) осіб, які ухиляються від відбування покарання, безвісно зниклих та інших категорій осіб, які розшуковуються відповідно до Інструкції (п.1.4.3.5);

7) ІІ «Пізнання» – автоматизований облік інформації у тому числі біометричних даних щодо осіб, які переховуються від органів влади, безвісно зниклих осіб, невпізнаних трупів та людей, які не можуть надати про себе будь-яку інформацію у зв'язку з хворобою або неповнолітнім віком. Ведення обліку регламентовано Інструкцією (п.1.4.3.5. та 1.4.3.13);

8) ІІ «Гартун» – автоматизований облік даних про транспортні засоби, які пересуваються шляхами загального користування та номерні знаки, які розшуковуються з будь-яких підстав у рамках кримінального або виконавчого провадження, стали засобом або предметом учиненого кримінального правопорушення, та інші відомості про транспорт, які можуть становити службовий інтерес для правоохоронних органів при з'ясуванні об'єктивних обставин у разі встановлення або запобігання факту порушень прав та свобод людини, гарантованих державою;

9) ІІ «Номерні речі» – автоматизований облік відомостей щодо речей, викрадених, вилучених з ознаками підробки, заборонених або обмежених в обігу у фізичних осіб, безгосподарних, знайдених або вилучених із камер схову вокзалів, аеропортів, зданих до органів поліції, які мають індивідуальні заводські (фабричні) номери;

10) ІІІ «*Культурні цінності*» – автоматизований облік даних щодо викрадених, вилучених культурних цінностей, що належать до об'єктів матеріальної і духовної культури та мають художнє, історичне, етнографічне та наукове значення, матеріали щодо яких зареєстровано органами поліції;

11) ІІІ «*Кримінальна зброя*» – автоматизований облік відомостей про викрадену, втрачену, вилучену, знайдену зброю, а також добровільно здану зброю із числа тієї, що незаконно зберігалася, незалежно від її технічного стану, що має індивідуальні заводські (фабричні) номери або номери деталей: нарізної, комбінованої, гладкоствольної, газової, пневматичної, стартової, сигнальної, під патрон Флобера, холодної, пристроїв для відстрілу патронів, споряджених гумовими чи аналогічними за своїми властивостями металевими снарядами не смертельної дії. Ведення обліку регламентовано Інструкцією (п.1.4.3.6); 12) ІІІ «*Зареєстрована зброя*» – автоматизований облік відомостей стосовно зброї, що має індивідуальні заводські (фабричні) номери, перебуває в користуванні громадян, підприємств, установ, організацій, господарських об'єднань, яким надано, відповідно до законодавства, дозвіл на її придбання, зберігання, носіння, перевезення, та яка обліковується органами поліції: нарізної, комбінованої, гладкоствольної, газової, пневматичної, холодної, пристроїв вітчизняного виробництва для відстрілу патронів, споряджених гумовими чи аналогічними за своїми властивостями металевими снарядами не смертельної дії. Ведення обліку регламентовано Інструкцією (п.1.4.3.6);

13) ІІІ «*Домашній арешт*» – автоматизований облік даних стосовно підозрюваних, обвинувачених, щодо яких застосовано запобіжний захід у вигляді домашнього арешту. Ведення обліку регламентовано Інструкцією, зазначеною у п.1.4.3.7;

14) ІІІ «*Документ*» – автоматизований облік відомостей про викрадені (втрачені) паспортні документи, інформацію щодо яких зареєстровано органами поліції за зверненнями громадян;

15) ІІІ «*Атриум*» – автоматизований облік даних стосовно осіб, звільнених з місць позбавлення волі, засуджених та тих, які притягаються до кримінальної відповідальності;

16) ІІІ «*Дактилоскопічний облік*» – автоматизований облік відомостей про дактилоскопічні карти, складені щодо осіб, затриманих за підозрою у вчиненні правопорушень (адміністративне затримання, затримання згідно з дорученням органів правопорядку, затримання осіб органами досудового розслідування, адміністративний арешт, домашній арешт), а також невідомих трупів та людей, які не можуть надати про себе будь-яку інформацію у зв'язку з хворобою або неповнолітнім віком;

17) ІІІ «*Аналітика*» – програмний комплекс аналітичних засобів забезпечує роботу генератора запитів та генератора звітів. Генератор запитів - уніфікована система пошукових та аналітичних сервісів для використання інформації з інформаційних ресурсів (тимчасових наборів даних, баз даних) поліції, МВС та інших органів державної влади для забезпечення службової діяльності працівників поліції відповідно до їх повноважень та наданого рівня доступу.

18) *Підсистема підтримки електронних цифрових підписів* – це програмні засоби, що розміщуються та функціонують на програмно-технічних потужностях ІПНП та забезпечують можливості накладання електронного цифрового підпису на документи, утворені в процесі оперативно-службової діяльності поліції в електронному вигляді та внесені до ІПНП, контролю за автентифікацією дій користувачів, які вносять будь-які зміни до системи ІПНП, використання ЕЦП для засобів криптографічного захисту інформації, взаємодії з центрами сертифікації ключів;

19) *ІІІ Аналітика ситуаційних центрів* – сукупність програмних модулів для формування узагальнених автоматизованих відомостей, інформаційно-аналітичних матеріалів з питань протидії злочинності, у тому числі за окремими видами кримінальних правопорушень та на території окремих регіонів, забезпечення публічного порядку та безпеки, протидії терористичній діяльності, ліквідації наслідків стихійного лиха тощо. Забезпечує узагальнення та моніторинг відомостей про кримінальні правопорушення, надзвичайні ситуації та інші події, які надходять з різних джерел за визначеними або пов'язаними параметрами – ознаками, джерелами, фактами, об'єктами, особами, які необхідні для підготовки та прийняття управлінських рішень у сфері забезпечення охорони прав і свобод людини, публічної безпеки і порядку, протидії злочинності та терористичній діяльності, надання відповідної інформації керівництву Національної поліції України та органам і підрозділам поліції. Функціонування підсистеми регламентовано Положенням (п.1.4.3.12);

20) *ІІІ ведення користувачів ІПНП* – забезпечує реалізацію таких функцій:

- реєстрація користувачів центрального ПТК;
- надання користувачам центрального ПТК прав доступу до програмних комплексів та інформаційних підсистем з відповідними «привілеями»;
- блокування, видалення (відміна), зміна «привілеїв» та редагування запису користувача центрального ПТК;
- перегляд системних журналів стосовно дій користувачів;
- підтвердження зміни повноважень користувача відповідно до підсистеми управління персоналом.

21) *ІІІ Кримінальна аналітика* – забезпечує доступ (інформаційну взаємодію) до інформаційних ресурсів окремим програмним засобам або формує необхідні інтерфейси, що використовуються для функціонування моделі поліцейської діяльності, керованої аналітикою «Intelligence Led Policing»;

22) *ІІІ Ведення класифікаторів* – призначена для редагування набору типових записів, що використовуються в інформаційних підсистемах та програмних комплексах центрального ПТК;

23) *ІІІ Конвертації інформації* – забезпечує перенесення та модифікацію даних між наявною та модернізованою системою ІПНП.

Формування у складі центрального ПТК ІПНП власних баз даних у сфері управлінських відносин, необхідних для виконання покладених на поліцію

повноважень, а також забезпечення щоденної діяльності поліції у сфері трудових, фінансових відносин, відносин документообігу:

1) *ІІІ фінансово-господарською діяльності* – автоматизована підсистема обліку однострою, службового автотранспорту та майна органів та структурних підрозділів Національної поліції;

2) *ІІІ «Рекрутинг»* – автоматизована система підбору кадрів, яка призначена забезпечувати проведення конкурсу на вакантні посади в НПУ та його інформаційне супроводження (окрім вакантних посад до підрозділів патрульної поліції);

3) *ІІІ «Кадри»* – автоматизована підсистема обліку персоналу НПУ;

4) *ІІІ «Архів»* – автоматизований облік відомостей про склад, зміст і місцезнаходження архівних фондів і (або) архівних документів, створених під час діяльності органів і підрозділів поліції;

5) *ІІІ СЕДО (Система електронного документообігу)* – призначена для документального забезпечення процесів управління та автоматизації діловодства та документообігу, здійснення контролю за виконавською дисципліною, забезпечення обробки електронних документів та за необхідності, документів у паперовому вигляді в діяльності Національної поліції та МВС. Ведення системи регламентовано Вимогами (п. 1.4.3.11);

6) *ІІІ Система електронної взаємодії державних електронних інформаційних ресурсів* – це окремий абонентський програмний модуль, що розміщується та функціонує на програмно-технічних потужностях ІІНП, призначений для автоматизації та технологічного забезпечення обміну електронними даними між суб'єктами владних повноважень з державними електронними інформаційними ресурсами під час надання адміністративних послуг та здійснення інших повноважень відповідно до покладених на них завдань шляхом використання сервіс-орієнтованої архітектури, що є інтерфейсами прикладного програмування доступу до державних електронних інформаційних ресурсів, побудованими згідно з єдиними вимогами, а також шляхом використання єдиних форматів, протоколів, довідників, шаблонів та класифікаторів. Функціонування підсистеми регламентовано Постановою (п.1.4.2.2);

7) *Call-центр Національної поліції* – автоматизована система прийому повідомлень на «гарячу» телефонну лінію 0800-500202. Забезпечує прийняття, фіксацію, оброблення та реєстрацію звернень громадян щодо питань, пов'язаних з діяльністю поліції (довідкова інформація, скарги на дії чи бездіяльність працівників поліції та повідомлення про правопорушення);

8) *ІІІ «102»* – автоматизована підсистема прийому повідомлень «102» за допомогою телекомунікаційних мереж. Забезпечує прийняття, фіксацію, оброблення та реєстрацію повідомлень про правопорушення та інші події, передачу інформації про них відповідним оперативно-диспетчерським службам для організації реагування на такі повідомлення. Функціонування підсистеми регламентовано Інструкцією (п. 1.4.3.2);

9) *ІІІ «Цунамі»* – автоматизована підсистема централізованого управління нарядами поліції. Забезпечує управління силами й засобами органів та

підрозділів поліції для реагування на повідомлення про правопорушення та інші події. Підсистема забезпечує інтеграцію прийнятих формалізованих повідомлень про правопорушення та інші події, інформацію про наявні сили поліції для здійснення реагування та їх статуси, їх взаємної геоінформаційної прив'язки, обміну інформацією з мобільними терміналами, що використовуються патрулями та іншими силами, інтерфейсів, аналітичних засобів для прийняття ефективних управлінських рішень диспетчерською службою. Функціонування підсистеми регламентовано Інструкцією (п. 1.4.3.9);

10) *Програмний модуль інтеграційної платформи ІПНП* для взаємодії інформаційних підсистем Національної поліції з регіональними сегментами систем забезпечення публічної безпеки і порядку (в рамках реалізації проектів «Безпечне місто»), інформаційними підсистемами та реєстрами інших ЦОВВ, у тому числі для здійснення розшуку осіб, транспортних засобів, забезпечення безпеки дорожнього руху та відеоаналізу інформації;

11) *Підсистема картографічної інформації* – програмні компоненти геоінформаційних підсистем, що необхідні для візуалізації інформації у вигляді електронних карт, автоматичної зміни зображеного образу об'єкта залежно від зміни його характеристик, масштабу та деталізації картографічної інформації для відображення даних;

12) *ІП «ДТП»* – автоматизований облік відомостей про дорожньо-транспортні пригоди, у тому числі фото-відеозображення з місця події, фіксування координат події на карті регіону (країни);

13) *ІП «Дозвіл БДР»* – автоматизований облік відомостей щодо дозволів на рух окремих категорій транспортних засобів, у тому числі небезпечних та негабаритних вантажів. Особливістю ІП є сервіси друку паперового вигляду дозвільного документа та перевірки оригінальності дозвільного документа за допомогою QR-коду із застосуванням будь-якого пристрою з функцією розпізнавання цього коду. Функціонування підсистеми регламентовано Правилами (п.1.4.3.17);

14) *ІП «ITT-Custody records»* – автоматизована підсистема, що забезпечує відстеження порядку тримання осіб в ізоляторах тимчасового тримання головних управлінь Національної поліції (ІТТ) для здійснення оперативного реагування на випадки порушення їх прав і законних інтересів, протиправних дій працівників поліції стосовно них, а також формування та ведення статистичних даних. Підсистема створюється відповідно до Меморандуму (п. 1.4.4);

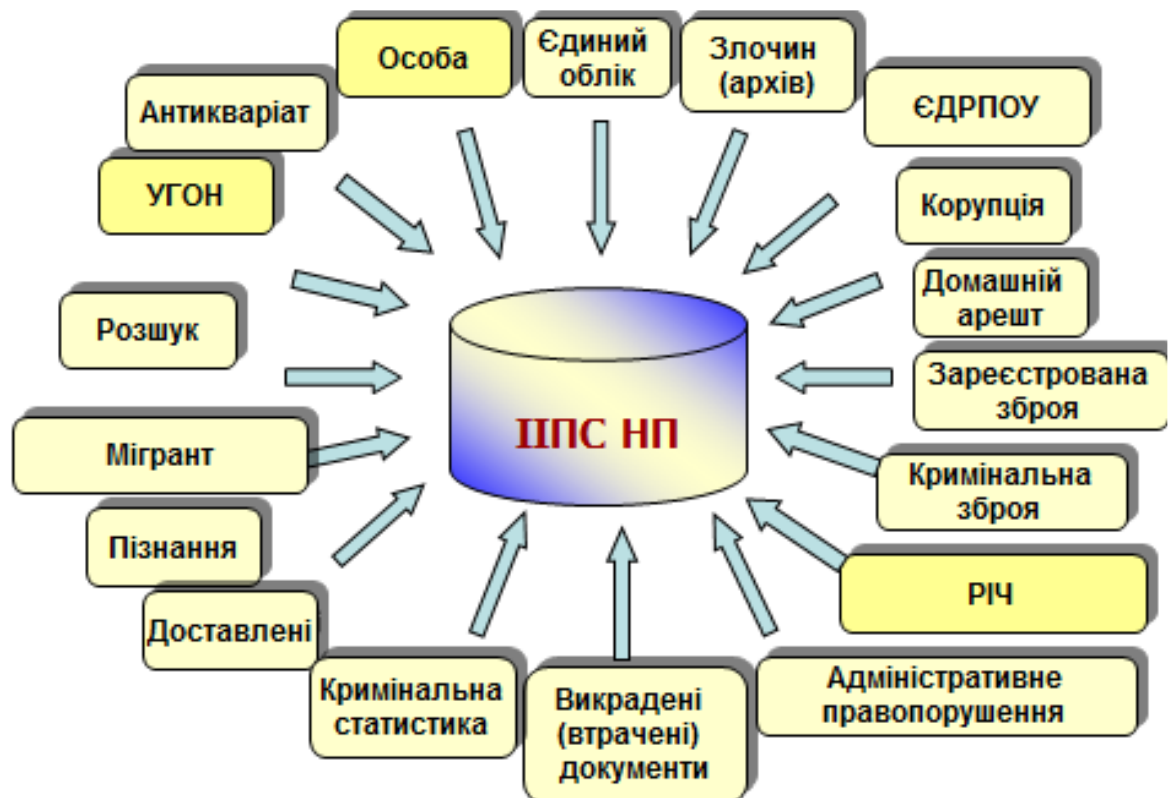
15) *Сегмент порталу взаємодії з ресурсами в мережі Інтернет* – програмний комплекс, що забезпечує підтримку мобільних додатків, призначених для інформування підрозділів поліції про правопорушення та події, поліпшення комунікації між органами поліції і громадськістю.

Розвиток програмного комплексу необхідно здійснювати на основі експериментального проекту мобільного додатку «Моя поліція» (здійснює опрацювання повідомлень та звернень громадян, які надійшли із застосуванням технологій для мобільних телефонних пристроїв (смартфонів).

За допомогою мобільного додатку передбачено опрацювання наступних основних функціональних можливостей:

- кнопка «SOS» використовується для відправлення екстреного виклику на спецлінію «102»;
- повідомлення про правопорушення (у тому числі з фото-, відео- та аудіофайлами);
- push-сповіщення – отримання користувачами важливої інформації від поліції (у тому числі про надзвичайні новини, орієнтування, перекриття руху під час проведення масових заходів тощо);
- «активний свідок» – дозволяє швидко знаходити свідків правопорушення, використовуючи потенціал мобільних платформ;
- карта відділень поліції та медичних закладів – можливість відшукати найближче відділення, куди можна звернутися за допомогою;
- інструкція спілкування з поліцейськими – як правильно діяти у тій чи іншій ситуації, а також як мають поводитися поліцейські;
- моніторинг роботи поліцейських – користувачі програми мають змогу оцінити роботу поліцейського за п'ятибальною шкалою, а також залишити анонімний відгук;
- актуальні новини поліції – можливість користувачів ознайомитися з новинами поліції.

Інтегрована інформаційно-пошукова система Національної поліції складається з наступних інформаційних підсистем (мал. 1)



Мал. 1. Інтегрована інформаційно-пошукова система Національної поліції

4. Система централізованого управління нарядами поліції

Система централізованого управління нарядами поліції (скорочено – система «ЦУНАМІ») являє собою комплекс апаратних та програмних засобів, а також персоналу, призначений для управління силами й засобами Національної поліції.

Дана система забезпечує користувачів необхідними інформаційними, технічними та аналітичними ресурсами для виконання функціональних обов'язків та прийняття ефективних управлінських рішень. Система фіксує, зберігає та робить доступними для аналізу та контролю повідомлення і результати реагування на них.

Мета впровадження системи «ЦУНАМІ» обумовлена необхідністю вдосконалення процесу організації діяльності з управління силами й засобами Національної поліції для ефективного реагування на повідомлення про злочини та події.

Організаційно система «ЦУНАМІ» складається з двох рівнів – міського та районного. До складу міського рівня організаційної структури входять ситуатійні центри, які діють у всіх обласних центрах України та м. Київ.

Ситуатійний центр – це підрозділ зі збору, опрацювання й аналізу інформації щодо рівня, структури і динаміки злочинності по всій Україні.

Основні компоненти системи «ЦУНАМІ»:

Організаційно-управлінський рівень

1.) Центр прийняття повідомлень – служба «102»

1.1. Служба «102»

1.2. Онлайн-сервіс 102kiev.com.ua

1.3. Чергова служба (чергові частини Головних управлінь, апарату Національної поліції)

2.) Диспетчерський центр управління

3.) Інформаційно-технічний супровід системи.

3.1. Геоінформаційна система (електронна карта міста).

3.2. Система супутникового GPS-позиціонування та мобільного комунікаційного обладнання.

3.3. Система відеоспостереження.

3.4. Система колективного відображення.

Виконавчий рівень

1.) Наряди управління патрульної поліції.

2.) Групи реагування патрульної поліції (ГРПП).

3.) Слідчо-оперативні групи.

4.) Наряди управління поліції охорони.

5.) Чергові частини управлінь, відділів поліції (а також УПО, УПП).

6.) Додаткові сили (дільничні офіцери поліції, працівники управління захисту економіки, кіберполіції, вибухотехнічної служби, кінологічного центру, спеціалісти НДЕКЦ тощо).

Система централізованого управління нарядами поліції (скорочено – система «ЦУНАМІ») являє собою комплекс апаратних та програмних засобів, а також персоналу, призначений для управління силами й засобами Національної поліції.

Мета впровадження системи «ЦУНАМІ» обумовлена необхідністю вдосконалення процесу організації діяльності з управління силами й засобами Національної поліції для ефективного реагування на повідомлення про злочини та події.

Досягнення зазначеної мети забезпечується виконанням таких завдань:

- оптимізація роботи нарядів патрульної поліції, слідчо-оперативних груп чергових частин;
- скорочення часу реагування на повідомлення громадян про злочини та події, попередженню правопорушень й затримання злочинців по «гарячих слідах»;
- здійснення оперативного контролю за своєчасністю і якістю реагування нарядами поліції на злочини та правопорушення, дотриманню законності під час виконання службових обов'язків працівниками поліції.

Скорочення часу реагування на повідомлення громадян про злочини та події відбувається за рахунок оптимізації відповідних інформаційних потоків.

Потоки інформації, які надходять в службу «102» по Україні, можна оцінити таким чином:

- загальне навантаження на службу «102» – близько 3 тис. викликів на добу;
- середній час дозвону заявника – 5–10 сек.;
- сумарний потік інформації на один пульт – до 280 звернень за добу.

Організаційно система «ЦУНАМІ» складається з двох рівнів – міського та районного.

До складу міського рівня організаційної структури входять ситуаційні центри, які діють у всіх обласних центрах України та м. Київ.

Створення системи ситуаційних центрів почалося разом зі створенням Національної поліції близько двох років тому. По-перше, було зрозуміло, що колишні чергові частини не відповідають сучасним вимогам, і, як результат, правоохоронці сильно програють у швидкості реагування. По-друге, збільшилася кількість звернень громадян. Ще кілька років тому протягом року до поліції зверталося близько 3 млн осіб, у 2017 році ця цифра перевищила за 7 млн. Свою роль зіграла патрульна поліція. Було створено патрульну поліцію, яка зараз працює в 33 містах. У сільських районах і невеликих містах розгорнуто групи реагування патрульної поліції, їх понад 1 тис. Також до системи реагування включено всю поліцію охорони, 450 нарядів, і всі слідчо-оперативні групи, які працюють у кожному відділі та відділку поліції. У зв'язку з цим виникла необхідність створення при Національній поліції ситуаційних центрів для відпрацювання всього масиву повідомлень та ефективного управління нарядами поліції.

Ситуаційний центр – це підрозділ зі збору, опрацювання й аналізу інформації щодо рівня, структури і динаміки злочинності по всій Україні. Є ситуаційний центр Нацполіції, де проводиться лише збір та опрацювання інформації, і ситуаційні центри в місті Києві та областях, у складі яких працює і служба «102».

Розглянемо типову робочу зміну ситуаційного центру обласного рівня:

- оперативний черговий – старший зміни центру;
- диспетчер (помічник) - обробляє інформацію внесену до ІПС ОНП забезпечує передачу спецповідомлень, контролює надходження електронної пошти;
- 10 операторів лінії «102», які приймають повідомлення від громадян та вводять її до електронної картки;
- 4 інспектори керування нарядами забезпечують ефективне управління силами та засобами задіяними по ОГП в області, інспектор системи відеоспостереження контролює відеоінформацію з відеокамер та передає для реагування або веде спостереження за масовими заходами в зоні розміщення камер;
- 2 інспектори з аналітики обробляють отриману інформацію про події проводять аналіз, готують аналітичні довідки, працюють з електронною картою подій;
- інспектор стаціонарного пульта моніторингу поведінки за особами до яких застосовано електронні засоби контролю (ЕЗК).

До складу районного рівня організаційної структури входять наступні підрозділи:

1. Чергові частини районних підрозділів Національної поліції.
2. Слідчо-оперативні групи.
3. Додаткові сили (дільничні інспектори поліції тощо).

У якості платформи для автоматизації служби «102» використовується сучасний цифровий call-центр (AWAYA), який інтегровано в існуючу інформаційну систему Національної поліції, що дозволило операторові одержувати інформацію про абонента ще до моменту підняття трубки, а саме:

- дані про власника телефонного номера;
- кількість дзвінків, які раніше надходили із цього номера та щодо яких подій;
- відстеження повторних викликів по вже зареєстрованій події;
- географічне місце (адресу) на електронній карті міста тієї події, про яку повідомлено;
- попередження про дзвінки абонентів, які внесено до окремого списку: психічно хворі, телефонні хулігани та інше.

При випадковому обриві зв'язку оператор сам може передзвонити абоненту. У разі, якщо оператор «102» виходить на технічну перерву, всі дзвінки автоматично та рівномірно розподіляються на інших операторів.

Інформаційна електронна картка «102».

APM 02 - Windows Internet Explorer

Агент № 4995843 Прізвище Вулиця Пошук Журнал 02 Картка "02"

Режим перерви

Подія: ГРАБІЖ Інстр.

Дата скоєння: 13.03.2009 01:23:00 скоєно год хв. тому

Место совершения (рус.)

Ул. АЗЕРБАЙДЖАНСКАЯ УЛ. Телефон: 445742151

Дом 2 кв. Статус: ГРОМАДЯНИН

Р-н ДНЕПРОВСКИЙ Прізвище: ВАСЬКОВСЬКИЙ

Н/п КИЕВ Ім'я: ОЛЕКСАНДР

Обл. По-бать...: ЮЛІАНОВИЧ

Дата нар. 03.01.1960 Знайти

Зміст:

НА ЗУП.ТРАМВАЯ БАКИНСЬКИХ КОМИСАРІВ 30 ХВ. ТОМУ 2-Є ЧОЛОВІКІВ ЗЗАДУ ВДАРИЛИ ПО ГОЛОВІ ТА ЗАБРАЛИ СУМКУ В ЯКІЙ БУЛИ ГРОШІ В СУМІ 5000 ГРН. ПРИКМЕТИ: ЗРІСТ 180, 30 РОКІВ, МІЦНОЇ СТАТУРИ, ОДЯГНЕНІ В ЧОРНІ КУРТКИ, ОДИН В КОМУФЛЯЖНИХ ШТАНАХ, ПОБІГЛИ ЗА РІГ БУДИНКУ. ЗАЯВНИК ЧЕКАЄ: ПРАЖСЬКА 29/1, КВ. 19.

Обслуговування:

Територія: ДНІПРОВСЬКЕ РУ Лінія роботи: ЧЧ

Документ: ЖРЗПЗ № 5047 від: 13.03.2009 01:32:00

Черговий: ФЕСЮК

ID: 373697

Введено: DEG0001 13.03.2009 01:26:59 ЗБЕРЕГТИ

Кореговано: WWW 10.04.2009 15:57:28 ДИСПЕТЧЕР

ІНФО

Інфо Інструкції Карта

Телефон

Телефонний номер 445742151

Всього дзвінків - 1 карток - 1

Сьогодні - 0

Останній - 13.03.2009 01:18:53 (п'ятниця)

Інформація

Прізвище - ВАСЬКОВСЬКИЙ ОЮ

місто - КИЕВ

вулиця - ПРАЖСКАЯ УЛ.

дом - 29/1

квартира - 19

дата встановлення - 16.07.03

Особа

- Знайдено 1 осіб

Адреса

- Знайдено 49 адрес
- Зброя на 3 адресах

Log

1/1 << < > >> + v - x ? M3 Документ сохранен!

Карта: 35028.94 , 50228.36 -- Изображение: 6 , 203 -- Коэфф. масштаба: 2.1725 Надежные узлы 100%

При заповненні електронної картки, оператор «102» здійснює попередню кваліфікацію події, про яку повідомлено. Заповнена оператором електронна картка відразу надходить до диспетчера-чергового відповідального за керування нарядами поліції в тому чи іншому районі міста.

Відповідне програмне забезпечення відображає інформацію про місце вчинення злочину на електронній карті міста.

Надалі електронна картка надходить до системи «ЦУНАМІ», і її обробленням займається диспетчер-черговий Головного управління (керує патрульними нарядами поліції для оперативного реагування на звернення) і оперативний черговий відповідного районного управління, до території якого відноситься звернення (реєструє звернення у журналі Єдиного обліку злочинів і правопорушень районного підрозділу Національної поліції).

Електронна картка, сформована оператором «102» одночасно відображається у чергового, що перебувають у диспетчерському центрі, та чергового відповідного райвідділу поліції на території якого відбувається подія (було вчинено правопорушення).

Зареєстровані звернення громадян зберігаються в електронному журналі.

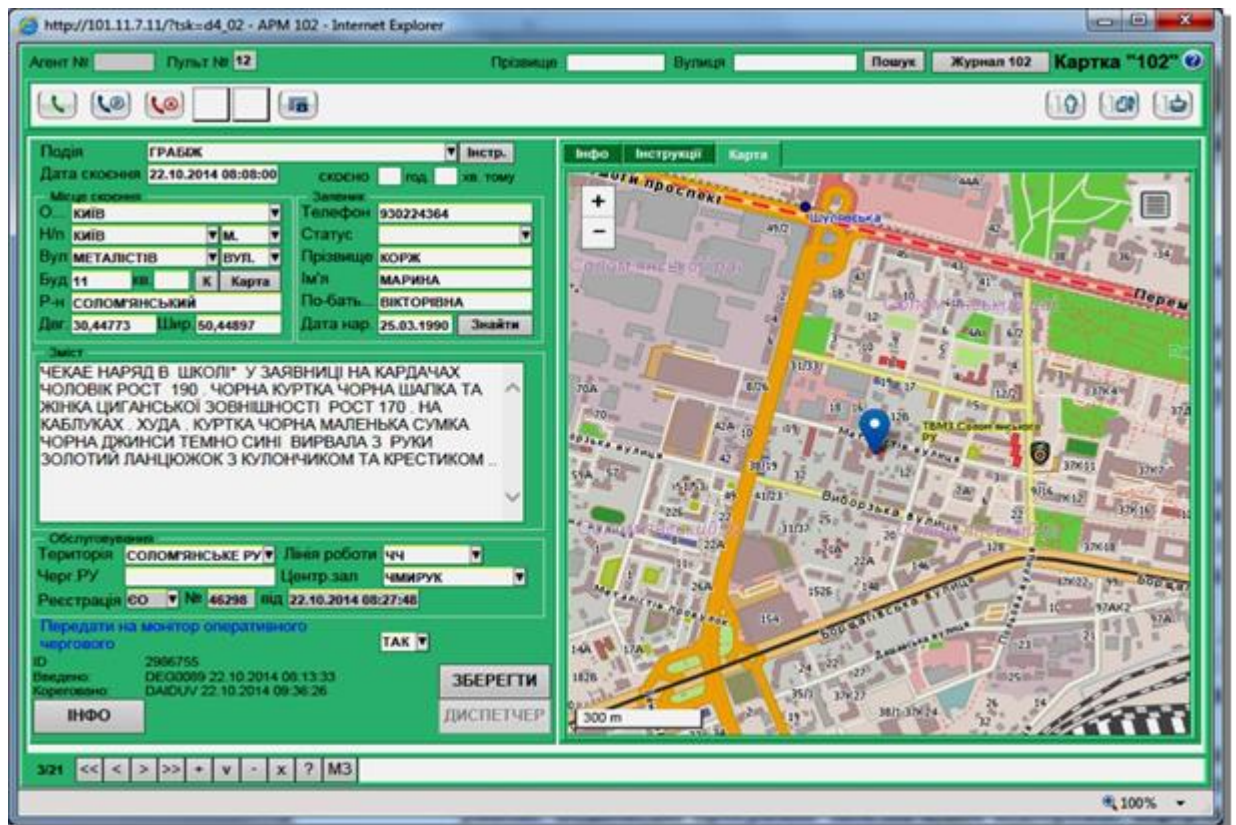
44	2990589	КОНФЛІКТ	24.10.2014 12:54:00	НЕВЕСТКА.ТЕЛ.950948330. СЕІНЧАС В КВАРТИРЕ КОНФЛІКТ С НЕІЗВЕСТНИМИ.	ДНІПРОВСЬКЕ РУ	СО 51933 від 24.10.2014 12:55 ()	ДНІПРО42 Довгань;
45	2990588	ЗВЕРНЕННЯ ІНФОРМАЦІЙНОГО ХАРАКТЕРУ	24.10.2014 12:54:00	-зі сторони вул.Богдана Хмельницького демонтаж тимчасової споруди,повідомляє представник благоустрою, ВІДМІНЯЄТЬ ВИКЛИ	ШЕВЧЕНКІВСЬКЕ РУ	Придано до події № 2990539	
46	2990587	КРАДІЖКА	24.10.2014 12:52:00	ПРОСИТЬ МІЛІЦІЮ ПОКВАПИТИСЬ.ЗАЯВНИЦЯ ПРАЦЮЄ В ДИТЯЧОМУ САДОЧКУ №28, ПОВІДОМИЛА, ЩО З КАБІНЕТУ ВКРАЛИ СУМКУ, В СУМЦІ ЗНАХОДИЛИСЯ ПАСПОРТ НА ІМ'Я ЗАЯВНИЦІ, ТА МОБІЛЬНИЙ ТЕЛЕФОН, БАНКОВСЬКІ КАРТКИ	ШЕВЧЕНКІВСЬКЕ РУ	ЕО 51933 від 24.10.2014 13:33 ()	СОГШЕВЧЕНКО47 СВ МОСКАЛЬОВ;
47	2990586	ДТП БЕЗ ПОТЕРПІЛИХ	24.10.2014 12:50:00	НА МОСТУ, В СТОРОНУ ЛЕПСЕ. ХІОНДАЙ АКЦЕНТ АА 8532 ІА, ТОЙОТА КАМРІ АІ 6800 СТ.	ШЕВЧЕНКІВСЬКЕ РУ	Придано до події № 2990534	
48	2990585	КРАДІЖКА З АВТО	24.10.2014 12:50:00	З АВТО РЕНО МАСТЕР АА9452ІА ВКРАЛИ КОВПАКИ З КОЛЕС	СВЯТОШИНСЬКЕ РУ	ЕО 47048 від 24.10.2014 12:52 ()	СОГРУ-72 ВАСІЛЬВ;
49	2990584	ДТП БЕЗ ПОТЕРПІЛИХ	24.10.2014 12:49:00	АВТО ХІОНДАЙ ВХ 5400 ВН, ДЕУ АА 5489 СМ	СВЯТОШИНСЬКЕ РУ	ЕО 47047 від 24.10.2014 12:51 ()	536 Гончарук;
50	2990583	ХУЛІГАНСТВО	24.10.2014 12:49:00	П'ЯНА ЖІНКА , ЗАЙШЛА ТА НЕ ХОЧЕ ПОКИДАТИ КВАРТИРУ.	СВЯТОШИНСЬКЕ РУ	ЕО 47046 від 24.10.2014 12:51 ()	АП-103 василишин; ВЕНБЕСТ94 КОНОВАЛ;
51	2990582	ШАХРАЙСТВО	24.10.2014 12:49:00	КОРП.ЗВ - 2 ЕТАЖ 1 КАБ. - ЖДЕТ ЗАЯВИТЕЛЬНИЦА. ФІРМА? ОБМАНУЛА ПРИ ТРУДОУСТРОЙСТВЕ НА 400ГРН. ПРОСИТЬ ПРИСКОРИТИ НАРЯД МІЛІЦІЇ	ШЕВЧЕНКІВСЬКЕ РУ	Придано до події № 2990578	
52	2990581	ПОЖЕЖА	24.10.2014 12:48:00	НА 101 ПОСТУПИВ ВИКЛИК ЗАДИМЛЕННЯ В 4 ПІД'ІЗДІ.	ШЕВЧЕНКІВСЬКЕ РУ	ЕО 51931 від 24.10.2014 13:28 ()	ШЕВЧЕНКО102 БЕЗПАЛЬКО;
53	2990580	ІНШІ ТІЛЕСНІ УШКОДЖЕННЯ	24.10.2014 12:41:00	ЗАЯВНИЦЯ ПОВІДОМИЛА, ЩО ЇЇ ПОБИВ МУЖ В АЛКОГОЛЬНОМУ СТАНІ	ДНІПРОВСЬКЕ РУ	ЕО 52982 від 24.10.2014 12:52 ()	ДІМ53 ТАРАН;
54	2990579	ЗВЕРНЕННЯ ІНФОРМАЦІЙНОГО ХАРАКТЕРУ	24.10.2014 12:40:00	ПРИЙМАЛЬНЯ.ХОЧЕ ПОВІДОМИТ ПРО СКОЄННЯ ЗЛОЧИНУ ГЕН. ПРОКУРОРОМ. УКРАЇНИ. ВИКЛИКА СОГ	ПЕЧЕРСЬКЕ РУ	Придано до події № 2990549	

Диспетчер системи «ЦУНАМІ» є оперативним черговим і куратором кожного конкретного райуправління поліції, відповідальним за організацію реагування на злочини та пригоди в районах. До функцій чергових-диспетчерів входить:

- управління нарядами поліції;
- отримання інформації з служби «102» та відстеження на електронній карті місць учинення правопорушень;
- передача даних про правопорушення на планшет конкретного патруля поліції;
- забезпечення відповідного патруля всією наявною інформацією, що знаходиться у відомчих інформаційних масивах, про заявника та адресу виїзду;
- координація роботи найближчих вільних нарядів поліції, які залучаються до розкриття злочину по «гарячих слідах», виїзду до заявника, на місце пригоди або в напрямку вірогідного переховування злочинця;
- контроль часу виїзду наряд) та відстеження результатів реагування на заяви та повідомлення громадян про злочини, прийняті рішення тощо.

Патруль одержує від диспетчера у формі електронного повідомлення основні дані із заяви, у тому числі номер заявника.

За результатами реагування диспетчер ставить відповідні відмітки. Інформаційна електронна картка залишається у диспетчера на контролі, поки не буде отриманий повний звіт про результати реагування на звернення.



При здійсненні планування розстановки сил та засобів, задіяних для охорони громадського порядку, в системі використовується криміналістичний аналіз, який відображає оперативну обстановку на території обслуговування Національної поліції в різних розрізах та геоінформаційною прив'язкою до місцевості.

В системі використовуються звіти та аналітичні форми наступного характеру:

- аналіз реєстрації подій та правопорушень в розрізі підрозділів Національної поліції;
- аналіз реєстрації подій та правопорушень в розрізі видів злочинів;
- аналіз реєстрації подій та правопорушень по часу скоєння;
- відомості про час призначення та час прибуття нарядів з моменту отримання повідомлення службою «102»;
- відомості про час прибуття СОГ на місце події;
- список завдань по часу прибуття/відпрацювання патрулів;
- кількість повторних викликів за період тощо.

Автоматизоване робоче місце диспетчера міського управління патрульної поліції забезпечує управління нарядами для реагування на прийняті злочини та події, а саме:

- відображає перелік подій, прийнятих оператором «102», які були вчинені в районі обслуговування;
- відображає дислокацію та стан роботи патрульних нарядів;
- інформує, у кольоровій гаммі, про послідовність реагування на подію;

- сигналізує про перевищення часових нормативів окремих етапів виконання завдання;
- в разі визначення телефонного номера заявника відображає накопичені дані по цьому номеру (за якою адресою встановлено, кількість та зміст попередніх звернень);
- надає можливість зв'язатись з оператором «102», який прийняв виклик;
- надає можливість зв'язатись з заявником для уточнення даних по події;
- в разі отримання ПІБ заявника надає всю наявну інформацію про особу з інтегрованого банку даних «АРМОР»;
- надає повну інформацію на адресу з інтегрованого банку даних «АРМОР»;
- інформує про повторність надходження інформації про подію;
- контролює реєстрацію події у журналі Єдиного обліку.

http://101.11.7.45/?tsk=d4_suzm_mon - Моніторинг АСУНМ - Windows Internet Explorer

Моніторинг роботи АСУНМ

00:19	ДТП БЕЗ ПОТЕРП...	10.04.09 17:27	СОЛОМ'ЯНСЬКЕ...	ДАІ	УЛ. УШИНСКОГО д.26	805	ПРИБ	00:02	
00:21	ДТП БЕЗ ПОТЕРП...	10.04.09 17:24	ДНІПРОВСЬКЕ РУ	ДАІ	БУЛЬВАР ДАРНИЦКИЙ д.9	803	ПРИБ	00:05	
00:21	ДТП БЕЗ ПОТЕРП...	10.04.09 17:24	ПОДІЛЬСЬКЕ РУ	ДАІ	УЛ. НАБЕРЕЖНО-КРЕЩАТИНСКА...	807	ПРИБ	00:03	
00:24	ДТП БЕЗ ПОТЕРП...	10.04.09 17:21	ДНІПРОВСЬКЕ РУ	ДАІ	НАБЕРЕЖНАЯ РУСАНОВСКАЯ	803	ПРИБ	00:08	
00:25	ІНША ПОДІЯ	10.04.09 17:21	ДЕСНЯНСЬКЕ РУ	ЧЧ	УЛ. МИЛЮТЕНКО д.12 кв.63	ГШР "КОНСУ...	ПІДТ	00:22	ЖОІ 4831
00:31	ХУЛІГАНСТВО	10.04.09 17:14	ДАРНИЦЬКЕ РУ	ЧЧ	УЛ. ЗАТИШНАЯ д.76	ДАРНИЦЯ 309	ПРИБ	00:05	ЖРЗПЗ 7289
00:36	ГРАБІЖ	10.04.09 17:10	ДНІПРОВСЬКЕ РУ	ЧЧ	УЛ. МИКИТЕНКО ИВАНА д.11А	ДНІПРО 19	ПІДТ	00:19	ЖРЗПЗ 7220
						ДНІПРО 21	ПІДТ	00:31	
						ДНІПРО 17	ВИК	00:25	
						БАР-550	ПІДТ	00:28	
						КОНСУЛ-111	ПІДТ	00:28	
00:42	ІНША ПОДІЯ	10.04.09 17:03	ДНІПРОВСЬКЕ РУ	Д...	УЛ. ПОПУДРЕНКО	803	ВИК	00:08	
00:44	ВИЯВЛЕННЯ ОПІЗ...	10.04.09 17:02	ДЕСНЯНСЬКЕ РУ	ЧЧ	УЛ. МИЛОСЛАВСКАЯ д.39/48 кв.88	КОНСУЛ-109	ПРИБ	00:31	ЖРЗПЗ 6133
						СОГ-59 ДАВИ...	ПРИБ	00:19	
01:00	КРАДІЖКА	10.04.09 16:45	ГОЛОСІВСЬКЕ РУ	ЧЧ	ПРОСП. ГЛУШКОВА АКАДЕМИКА ...	СОГ РУ	ПІДТ	00:51	ЖРЗПЗ 4037
01:22	ПОВІДОМЛЕННЯ Л...	10.04.09 16:24	ДНІПРОВСЬКЕ РУ	ЧЧ	ПРОСП. ВАТУТИНА ГЕНЕРАЛА д.2...	ДНІПРО 43	ВИК	01:17	ЖРЗПЗ 7217
						АП 53 ДІМ БУ...	ПІДТ	01:00	
01:35	КРАДІЖКА	10.04.09 16:10	ДНІПРОВСЬКЕ РУ	ЧЧ	УЛ. МАЛИШКО д.21Б кв.144	СОГ 69	ПІДТ	01:31	ЖРЗПЗ 7215
01:58	ХУЛІГАНСТВО	10.04.09 15:47	ДНІПРОВСЬКЕ РУ	ЧЧ	НАБЕРЕЖНАЯ РУСАНОВСКАЯ д.10	БАР-570	ПІДТ	01:54	ЖОІ 5221
02:01	СІМЕЙНА СВАРКА	10.04.09 15:44	ДНІПРОВСЬКЕ РУ	ЧЧ	БУЛЬВАР БУЧЫИ АМВРОСИЯ д.4 ...	ДІМ 54	ПІДТ	01:54	ЖОІ 5220
02:12	КРАДІЖКА	10.04.09 15:33	ДНІПРОВСЬКЕ РУ	ЧЧ	ПРОСП. БРОВАРСКОЙ	СОГ 90	ПІДТ	01:28	ЖРЗПЗ 7214

Обслуговування районів

Орган	ЧЧ	ДАІ
ГОЛОСІВСЬКЕ РУ	1	2
ДАРНИЦЬКЕ РУ	1	2
ДЕСНЯНСЬКЕ РУ	1	2
ДНІПРОВСЬКЕ РУ	1	2
ОБОЛОНСЬКЕ РУ	0	2
ПЕЧЕРСЬКЕ РУ	0	2
ПОДІЛЬСЬКЕ РУ	0	2
СВЯТОШИНСЬКЕ РУ	0	2
СОЛОМ'ЯНСЬКЕ РУ	0	2
ШЕВЧЕНКІВСЬКЕ РУ	0	2
УО МЕТРОПОЛІТЕНУ	0	0
ІНШІ ОВС	0	0

Дзвінки операторам 02

№ Працівник	Дзвінкі	Прийнято	Картки
1 Всього	1043	951	398
2 Тарасюк Г.Г.	187	174	56
3 Залевська Л. С.	176	148	61
4 Грусевич І.Ю.	158	137	60
5 Завадська Л. В.	137	126	58
6 Левківський Ю. В.	119	108	56
7 Кривошея В.Г.	119	115	43
8 Панчихін І. С.	79	76	41
9 Кривда В. М.	68	67	23

Розподіл подій 02

№ Подія	к-сть
1 Всього	412
2 ДТП БЕЗ ПОТЕРПІЛИХ	154
3 ІНША ПОДІЯ	90
4 КРАДІЖКА	56
5 ХУЛІГАНСТВО	27
6 НАВМИСНЕ ПОШКОДЖ. МАЙНА	21
7 СІМЕЙНА СВАРКА	20
8 ГРАБІЖ	15
9 НЕЗАКОННА ТОРГІВЕЛЬНА ДІЯЛЬНІСТЬ	7
10 ПОВІДОМЛЕННЯ ЛІКАРЯ	5
11 ІНШИЙ ЗЛОЧИН	4
12 ЗАВОЛОДІННЯ АВТОТРАНСПОРТОМ	2
13 ДТП З ПОТЕРПІЛИМИ	2
14 РАПТОВА СМЕРТЬ	2

Готово

Надежные узлы

100%

Система в автоматичному режимі на протязі 30 хв. (якщо черговий самостійно не здійснить реєстрацію раніше) проводить реєстрацію звернення з картки «102» в електронний журнал «Єдиного обліку» (ЄО) та приєднує картку «102» до картки ЄО як джерело початкової інформації, що перешкоджає укріптю злочинів на стадії їх кваліфікації в районних управліннях, оскільки

оператор «102» та диспетчер відокремлені від впливу керівників територіальних органів.

Наряди патрульної поліції:

- відпрацьовують завдання, що надійшли від чергового-диспетчера;
- фіксують виконання етапів завдання за допомогою логістичного мобільного пристрою;
- надають короткий рапорт про виконання завдання (про результати реагування на звернення);
- взаємодіють з іншими патрулями з метою розкриття злочинів по «гарячих слідах».

Геоінформаційна система (електронна карта міста) використовується для візуального відображення на електронній карті міста місць учинення злочинів, усіх мобільних патрульних нарядів, оснащених GPS-приймачами, які в цей період часу виконують службові обов'язки.

Геоінформаційна система з відповідним програмним забезпеченням допомагає вирішити наступні завдання:

- планування і розміщення сил та засобів Національної поліції на підлеглій території, маршрутів та зон патрулювання (на підставі накопиченої статистики стосовно місць скоєння злочинів - CrimeAnalytics);
- контроль за діяльністю нарядів поліції з використанням системи супутникового позиціонування GPS;
- організація взаємодії нарядів поліції;
- при необхідності надає інтерактивну рекомендацію-підказку щодо призначення патрулів на подію для реагування;
- інтерактивний аналіз і розбір дій підрозділів Національної поліції при реагуванні на правопорушення;
- можливість відображення маршруту (треку) руху автопатруля;
- виявлення патрулів, треки яких перетинали визначену територію у визначений час;
- графічне відображення стану оперативної обстановки та статистичного аналізу по видах злочинів.



Система супутникового GPS-позиціювання та мобільного комунікаційного обладнання. Необхідною складовою системи є оснащення патрулів системою супутникового GPS-позиціювання та мобільного комунікаційного обладнання з можливістю підключення до інформаційних обліків Національної поліції. Таке обладнання дозволяє відслідковувати місцезнаходження патруля, напрямки його руху та статус на даний час (зайнятий, вільний, на перерві).

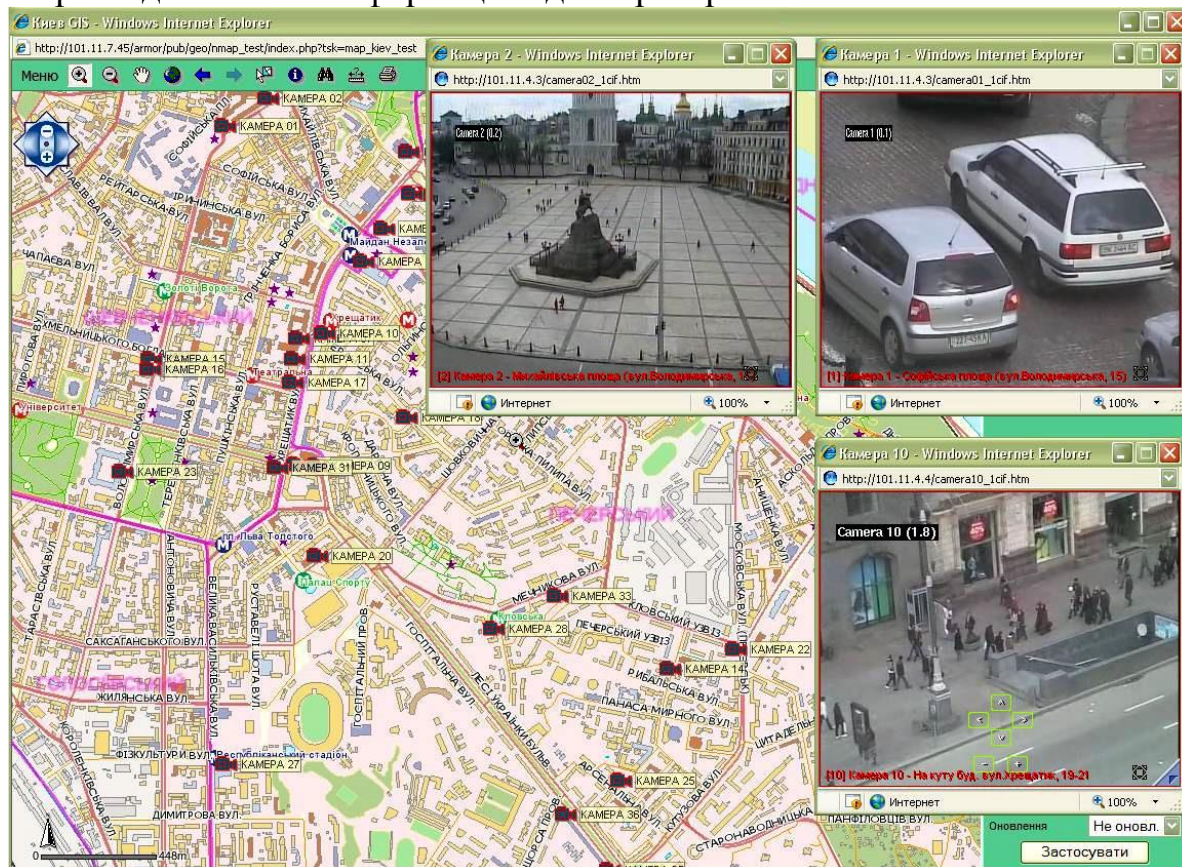
В салоні автопатруля встановлюється спеціальний блок керування та відображення. Цей пристрій фактично є портативним комп'ютером, який дозволяє отримувати завдання від диспетчера-чергового в електронному вигляді, автоматично прокладати маршрут до місця скоєння, надає можливість інформувати диспетчера, що наряд приступив до виконання завдання, прибув на місце пригоди, виконав завдання або завершив патрулювання. Також цей пристрій забезпечує доступ до інформаційної системи «АРМОР», що дозволяє працівнику поліції безпосередньо на місці при необхідності отримати інформацію з інформаційних обліків Національної поліції.

З моменту підтвердження прийому завдання система розпочинає супроводження руху наряду до місця події. В разі значного відхилення від нормативів часу реагування на той чи інший злочин система автоматично повідомляє про це чергового та пропонує додатково направити на місце події інший патруль.

З моменту підтвердження прийому завдання система розпочинає супроводження руху наряду до місця події. В разі значного відхилення від нормативів часу реагування на той чи інший злочин система автоматично

повідомляє про це чергового та пропонує додатково направити на місце події інший патруль.

Система відеоспостереження. Метою впровадження такої системи є необхідність оперативного візуального контролю за основними криміногенними місцями, вулицями, площами, транспортними потоками, а також перегляд записаної інформації під час розкриття злочинів.



5. Висновки

Таким чином, телекомунікаційна мережа доступу системи ПНП є сукупність технічних і програмних засобів, призначених для обміну інформацією між складовими системи. Для захисту інформації, що обробляється органами (підрозділами) поліції в системі ПНП, використовуються канали Єдиної цифрової відомчої телекомунікаційної мережі Міністерства внутрішніх справ України, а при використанні відкритих каналів - засоби захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації.

Комплексна система захисту інформації з підтвердженою відповідністю – взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації.

Завданням комплексної системи захисту інформації є забезпечення конфіденційності (у разі обробки інформації з обмеженим доступом), цілісності, доступності інформації в системі ПНП шляхом здійснення заходів, спрямованих на захист інформації від несанкціонованих дій (у тому числі з

використанням комп'ютерних вірусів), які можуть призвести до її випадкової або умисної модифікації чи знищення.

Контроль за дотриманням вимог законодавства України в сфері захисту інформації під час використання ПНП здійснює керівник підрозділу, де експлуатується центральний програмно-технічний комплекс системи.